

**July 27, 2012**

**ILHIE Invited Public Comment**

**Panel 5: Patient Choice and Consent: Operational Protocols**

***What is the best way to inform patient choice regarding the risks and benefits of HIEs? Should providers have to discuss HIEs with patients such that “meaningful choice” is obtained? Or do “Notice of Privacy Practices” accompanied by informative website disclosures suffice?***

With regard to the granting of consent for the exchange of health information, two general models have emerged for HIE’s to choose from, each with its own particular application.

Upon first consideration the "opt-in" model appears to provide patients with the greatest degree of “meaningful choice”.

A patient’s “meaningful choice” means that choice is:

1. Made with advance knowledge/time;
2. Not used for discriminatory purposes or as condition for receiving medical treatment;
3. Made with full transparency and education;
4. Commensurate with circumstances for why HIE is exchanged;
5. Consistent with patient expectations;
6. Revocable at any time.<sup>1</sup>

To avoid interfering with an individual’s access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities. The core health care activities of “Treatment,” “Payment,” and “Health Care Operations” are defined in the Privacy Rule at 45 CFR 164.501.

A covered entity may voluntarily choose, but is not required, to obtain the individual’s consent for it to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers. A “consent” document is not a valid permission to use or disclose protected health information for

---

<sup>1</sup> Department of Health & Human Services, (2012, March, 22). Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, Program Information Notice. Document Number: ONC-HIE-PIN 003. Office of the National Coordinator for Health Information Technology, Washington, DC.

a purpose that requires an “authorization” under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of protected health information.<sup>2</sup>

The “Opt-in” model prohibits the HIE network from automatically including a patient's information in the data that is passed from provider to provider via the HIE without the patient authorizing direct general consent for that express purpose. A variation of the “opt-in” model; “opt-in with restrictions,” introduces additional policies and procedures that allow the patient to limit or restrict disclosure of specific sensitive health information.

Although the opt-in method enables patients have maximum control of their data, it presents the HIE with significant administrative obstacles. To successfully oversee the process, each individual data provider would be required to collect consent from each patient, which burdens providers with another round of paperwork. Ensuring those select restrictions requires development and implementation of a complex technical process.

Implementing the processes to manage the restrictions is a task that could take months or even years to realize. The “opt-in” consent process as envisioned would require that a trust relationship be established. To be successful, this trust relationship must be built upon a formal consent documentation process; formal staff training, consumer education, community outreach, and stakeholder buy in. Primary among the challenges facing the HIE include:

- The lack of formally defined consensus based confidentiality codes denoting sensitive data.
- The challenge of training registration staff to deliver a consistent “meaningful choice” “opt-in” consent message.
- The lack of consistent patient health literacy levels.
- The lack of consistent patient technology literacy levels.

The alternate consent model to “opt-in” is considered to be the “opt-out” consent model. Considered by many to be the method that offers the contributing data provider an easier means to supplying the HIE with sufficient patient data, a good number of stakeholders are concerned that it would not give patients enough control over their information.

In an opt-out model, a data provider passes all patient health information that is not otherwise restricted via an HIE to participating providers. In an “opt-out” model it is the responsibility of the HIE to only block access to the patient data if the patient has chosen to opt out of the exchange.

A variation of the “opt-out” model; “opt-out with exceptions” model, allows patients initially included in the HIE to either exclude themselves entirely or include only specified or partial information. Implementation of an “opt-out with exceptions” model would require the HIE to be

---

<sup>2</sup> Office of Civil Rights, Uses and Disclosures of Treatment, Payment, and Health Care Operations. 45 CFR 164.506. Retrieved on July 25, 2012 from: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html>

technically and operationally ready to address the exclusion of specific information on a patient-by-patient basis.

Although, the “opt-out method” is often considered by some stakeholders to ignore patient control by not providing sufficient granularity of choice, if implemented properly, the “opt-out” consent model could provide a less administratively burdensome solution for both participating providers and the HIE organization; while still allowing patients to exercise their choice regarding the sharing of their own data.

How the “opt-out” consent process would support patient “meaningful choice” consent:

- Each time the patient visits providers participating in the HIE network they are given the opportunity to change their consent status.
- Patients receive an educational brochure containing a form they can complete if they elect not to participate.
- Individuals wishing to opt-out of the HIE can either visit the HIE Web site or contact the patient support line.
- Formal consent model training is provided at data provider sites to ensure that patients are provided with adequate information to make an informed decision regarding access to their data.
- Patients were provided with multiple options at the point of care to modify their consent status.
- Regardless of the method the patient chooses to make their consent preference known, all consent preferences are routed directly to the main HIE organization. Once received, the opt-out is processed within one business day, placing a block on the patient's information.
- For administrative purposes the HIE retains access to a minimal amount of patient demographic information, but no clinical information or further personal data are accessible. The small amount of data that remains visible in the master patient index—name, gender, birth date, and consent status—allows physicians to effectively and accurately search for and identify patients to determine if their data are accessible in HIE.
- On a weekly basis the HIE mails a confirmation letter to all individuals who have opted out during the previous week. The letter confirms their opt-out status and provides information regarding the HIE and the benefits of participation. Also provided are instructions on how the patient can reverse his or her consent status.
- An electronic track process is in place to track patients who decide to opt back into the HIE. All changes are audited to confirm that patients do indeed intend to opt in. Once the HIE staff confirm the request, the patients are mailed a letter of confirmation.
- Office process cross checks are performed to validate the accuracy of the patients consent preference.
- An audit of the “meaningful choice” consent process is performed on opt-out requests by provider location to determine if front line consent specialists require further education.
- Staff turnover at the provider sites warrants regular training to emphasize the importance of informing patients of their rights and the benefits of participation.
- In addition, HIE consent communication specialists monitor for variation in office workflow processes to ensure compliance with “meaningful choice” opt-out policies and procedures.

***Should all consents be written or can consent be obtained orally?***

An emergency disclosure under § 164.512(j)(1)(i) to avert an imminent threat to safety is lawful only if made in the good faith belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and to a person reasonably able to prevent or lessen the threat. If these conditions are met, no further verification is needed. In such emergencies, the covered entity is not required to demand written proof that the person requesting the protected health information is legally authorized. Reasonable reliance on verbal representations is appropriate in such situations.

ESIGN (Electronic Signatures in Global and National Commerce) Act & UETA (Uniform Electronic Transactions Act) allow for electronic signature in the form of an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.<sup>3</sup>

***Once consent is validly obtained, is it valid for an unlimited duration of time?***

The authorization identifies the time period for which the authorization is effective and expiration date or event.

The Department of Health and Human Services offered the following guidance about authorizations:

"The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire 'one year from the date the Authorization is signed,' 'upon the minor's age of majority,' or 'upon termination of enrollment in the health plan.'

"An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event."<sup>4</sup>

***(c) Implementation specifications: Core elements and requirements.***

(1) *Core elements.* A valid authorization under this section must contain at least the following elements:

---

<sup>3</sup> Electronic Signatures in Global and National Commerce Act, (2000, June, 30). Public Law 106-229,

Retrieved on July from: <http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf>

<sup>4</sup> Department of Health and Human Services. "Must an Authorization Include an Expiration Date?" September 24, 2003. [www.hhs.gov/hipaafaq/use/476.html](http://www.hhs.gov/hipaafaq/use/476.html).

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.<sup>5</sup>

***Or can it be revoked after a certain amount of time?***

Authorization contains a statement informing the individual regarding the right to revoke the authorization in writing and a description how to do so.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by §164.520, a reference to the covered entity's notice.<sup>6</sup>

***If consent can be revoked how should providers reconcile conflicting patient consents?***

A formal consent directive application allows users to create, store, amend, and replace a consumer preference; transmit the preference electronically; allow for individual providers and other exchange participants to view the preference; apply the preference to an individual health record; transmit an update of the preference; reconcile conflicting preferences; maintain an audit log of the preference; and classify data.<sup>7</sup>

---

<sup>5</sup> U.S. Department of Health and Human Services Office for Civil Rights, HIPAA Administrative Simplification, 45 CFR Parts 160, 162, and 164.

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf>

<sup>6</sup> U.S. Department of Health and Human Services Office for Civil Rights, HIPAA Administrative Simplification, 45 CFR Parts 160, 162, and 164.

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf>

<sup>7</sup> HHS-ONC. *Consumer Preferences Draft Requirements Document*, October 5, 2009, at 34.

Available at:

[http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS\\_0\\_10779\\_891071\\_0\\_0\\_18/2009](http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10779_891071_0_0_18/2009)